(19) FEDERAL REPUBLIC OF GERMANY

GERMAN PATENT AND TRADEMARK OFFICE

(12) Unexamined Patent Application

(10) DE 198 16 572 A1

(51) Int. Cl.[6]: G 06 K 19/00

(21) Application No.: 198 16 572.2
(22) Filed: April 7, 1998
(43) Date Opened to Inspection: October 14, 1999

DE 198 16 572 A1

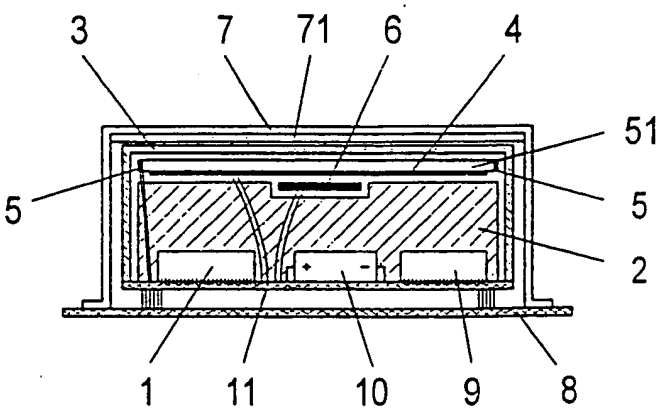
(71) Applicant:
Francotyp-Postalia AG & Co., 16547 Birkenwerder, DE

(72) Inventor:
Roussos, Georges, Dr., 10625 Berlin, DE

The following information has been taken from the documents submitted by the applicant

(54) Arrangement for a security module

(57) Arrangement for a security module for preventing the reading out or the unauthorized manipulation of security-related data.
Such modules are used, for example, in ASICS in franking machines or in automated teller machines.
The purpose is an improvement of the manipulation security. In accordance with this task, x-ray examinations are to be prevented, and attempts to drill it open or grind it open are to be without success.
In accordance with the invention, the security module 1 is surrounded by at least one x-ray absorbing enclosure 2 and is provided with means 4, 5, 6 for the purposeful manipulation of security-related data in the event of mechanical intervention and/or x-ray irradiation.



DE 198 16 572 A1

Patent Claims

1. Arrangement for a security module for preventing the reading out or the unauthorized manipulation of security-related data, **characterized in that** the security module (1) is surrounded by at least one x-ray absorbing enclosure (2) and
is provided with means (4, 5, 6) for the purposeful manipulation of security-related data in the event of mechanical intervention and/or x-ray irradiation.
2. Arrangement according to Claim 1, characterized in that the enclosure (2) is made of lead.
3. Arrangement according to Claim 1, characterized in that the enclosure (2) is made of a cast resin with an x-ray absorbing filler material made of lead and copper compounds plus optional additional filler materials.
4. Arrangement according to Claim 3, characterized in that a mixture of 85% minium -Pb_3O_4- and 15% cuprite -Cu_2O- is used, and as optional additional filler materials, quartz powder, glass beads or glass fibers.
5. Arrangement according to Claim 1, characterized in that the security module (1) is surrounded by an additional opaque enclosure (3), and
placed in the transition region between this enclosure (3) and the x-ray absorbing enclosure (2), are, optionally, a meandering electrical conductor (4) or a light detector (5) along with an optical fiber light guide (51) or an x-ray detector (6) or combinations of same, which are electrically connected with the security module (1) either directly or via a manipulation circuit (9).
6. Arrangement according to Claims 1 and 5, characterized in that the enclosure (3) is surrounded by an x-ray absorbing housing (7) which is placed on a circuit board (8) which is electrically connected with the security module (1).
7. Arrangement according to Claim 5, characterized in that the manipulation circuit (9) is electrically connected with the security module (1) only when the latter is in an electrically dead state.

In addition, 1 page(s) of drawings

---

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 16 572 A 1**

(51) Int. Cl.[6]: G 06 K 19/00

(21) Aktenzeichen: 198 16 572.2
(22) Anmeldetag: 7. 4. 98
(43) Offenlegungstag: 14. 10. 99

DE 198 16 572 A 1

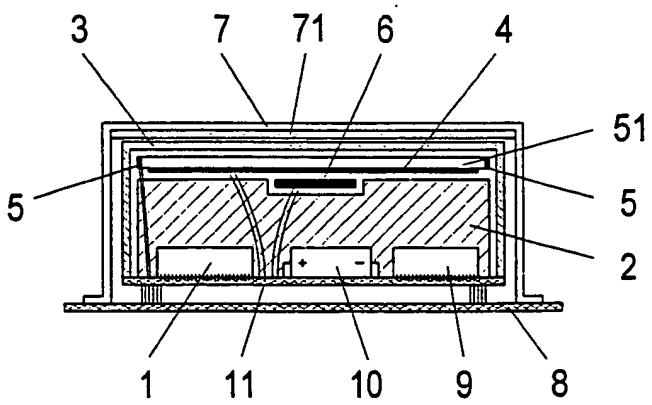
(71) Anmelder:
Francotyp-Postalia AG & Co., 16547 Birkenwerder, DE

(72) Erfinder:
Roussos, Georges, Dr., 10625 Berlin, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Anordnung für einen Sicherheitsmodul

(57) Anordnung für einen Sicherheitsmodul zur Verhinderung des Auslesens oder der unberechtigten Manipulation sicherheitsrelevanter Daten.
Ein derartiger Modul wird beispielsweise in ASICs in Frankiermaschinen oder in Geldautomaten eingesetzt.
Zweck ist eine Verbesserung der Manipulationssicherheit.
Aufgabengemäß sollen Röntgenuntersuchungen verhindert werden und Versuche mittels Aufbohren oder Aufschleifen erfolglos sein.
Erfindungsgemäß ist der Sicherheitsmodul 1 von mindestens einer Röntgenstrahlen absorbierenden Hülle 2 umgeben und mit Mitteln 4, 5, 6 zur gezielten Manipulation sicherheitsrelevanter Daten bei mechanischem Eingriff und/oder Röntgenbestrahlung versehen.



DE 198 16 572 A 1

Beschreibung

Die Erfindung betrifft eine Anordnung für einen Sicherheitsmodul insbesondere zur Verhinderung des Auslesens oder der unberechtigten Manipulation sicherheitsrelevanter Daten. Diese Daten können sicherheitsrelevante Teile eines Maschinenprogramms, Guthabenwerte oder andere sicherheitsrelevante Funktionen betreffen.

Ein derartiger Modul wird beispielsweise in ASICS in Frankiermaschinen oder Chipkarten für den Geldverkehr oder in Geldautomaten eingesetzt.

Zum allgemeinen Schutz und zum Schutz gegen Manipulationen wird der Sicherheitsmodul üblicherweise mit einer aushärtenden Vergußmasse umgeben, siehe EP 0 717 370 A2. Die Vergußmasse ist in der Regel ein Epoxydharz oder ein anderer geeigneter Plast.

Damit werden Manipulationen zwar erschwert, jedoch nicht verhindert. Um Manipulationen an einem derartigen Sicherheitsmodul vornehmen zu können, würde man zunächst denselben einer Röntgenuntersuchung unterziehen und anschließend an den für einen Zugang geeigneten Stellen aufschleifen oder aufbohren.

Weiterhin ist noch eine Beeinflussung über die elektrischen Anschlüsse möglich.

Eine andere bekannte Schutzmaßnahme besteht darin, den Sicherheitsmodul mit einer Folie mit einem mäanderförmigen Leiter hoher Packungsdichte zu umschließen und mit diesem elektrisch zu koppeln, siehe Bennet Yee "Using Secure Coprncessors" May 1994 CMU-CS-94-149, School of Computer Science Carnegie Mellon University Pittsburgh, page 7.

Der Leiter wird von einer Langlebensdauerbatterie gespeist. Bei Durchtrennung an irgendeiner Stelle werden der Stromkreis unterbrochen und infolgedessen die sicherheitsrelevanten Daten im Sicherheitsmodul gezielt manipuliert bis hin zur vollständigen Löschung derselben.

Zweck der Erfindung ist eine Verbesserung der Manipulationssicherheit.

Der Erfindung liegt die Aufgabe zugrunde, eine Anordnung zu schaffen die bewirkt, daß Röntgenuntersuchungen verhindert werden und separate Versuche mittels Aufbohren oder Aufschleifen nicht zum gewünschten Erfolg führen.

Erfindungsgemäß wird diese Aufgabe gemäß dem Hauptanspruch gelöst. Weitere vorteilhafte Merkmale der Erfindung sind den Unteransprüchen zu entnehmen.

Aufgrund der fakultativen Staffelung von Schutzhüllen und Detektoren werden je nach Bedürfnis und Aufwandsberechtigung ein sicherer Schutz gegen unberechtigte Manipulationen erreicht.

Die Erfindung wird nachstehend am Ausführungsbeispiel näher erläutert.

In der Figur ist ein Längsschnitt durch eine erfindungsgemäße Anordnung dargestellt.

Zur Vereinfachung und zum leichteren Verständnis ist die Darstellung schematisiert ausgeführt.

Gemäß **Fig. 1** besteht die erfindungsgemäße Anordnung aus:

- einem Sicherheitsmodul **1** nebst Manipulationsschaltung **9** und Batterie **10**, die gemeinsam auf eine Modulplatine **11** aufgesetzt und elektrisch miteinander verknüpft sind,
- einer die vorgenannten Baugruppen umgebenden Röntgenstrahlen absorbierenden Hülle **2**
- einem Röntgenstrahlen-Detektor **6**, einem mäanderförmigen elektrischen Leiter **4** und mindestens einem Lichtdetektor **5**, der mit einem Lichtleiter **51** gekoppelt ist, und die alle elektrisch mit der Modulplatine **11** verbunden sind,
- einer weiteren, lichtundurchlässigen Hülle **3** und
- einem die vorgenannten Bauteile umgebenden, Röntgenstrahlen absorbierenden Gehäuse **7**, das auf eine Platine **8** aufgesetzt ist die wiederum elektrisch mit der Modulplatine **11** verbunden ist.

Die Manipulationsschaltung **9** ist so beschaffen beziehungsweise programmiert, daß im Störungsfall sicherheitsrelevante Daten in vorgegebener Weise so manipuliert werden, daß der Sicherheitsmodul nicht mehr ordnungsgemäß arbeitet. Die bewußte Manipulation kann auch darin bestehen, das alle sicherheitsrelevanten Daten gelöscht werden. Die Batterie **10** dient zur Stromversorgung des mäanderförmigen Leiters **4** sowie der Manipulationsschaltung **9** und ist als Langlebensdauerbatterie ausgeführt.

Die Hülle **2** besteht aus einem Gießharz, der mit einem Röntgenstrahlen absorbierenden Füllstoff aus Blei- und Kupferlegierungen sowie wahlweise weiteren Füllstoffen versetzt ist. Der erste Füllstoff ist vorzugsweise eine Mischung aus 85% Mennige -Pb_3O_4- und 15% Cuprit -Cu_2O-. Als weitere Füllstoffe sind wahlweise Quarzpulver, Glaskugeln oder Glasfaser eingesetzt.

Die Hülle **2** kann alternativ auch als Bleimantelgehäuse ausgeführt sein.

Der Röntgenstrahlen-Detektor **6** außerhalb der Hülle **2** ist mit der Modulplatine **11** und über dieselbe mit der Manipulationsschaltung **9** oder mit dem Sicherheitsmodul **1** direkt elektrisch verbunden.

Dasselbe trifft auf den mäanderförmigen Leiter **4** und den Lichtdetektor **5** zu.

Die Hülle **3** ist lediglich als lichtundurchlässiges Gehäuse ausgeführt, mit dem zusätzlich zu seiner Hauptfunktion – bei Öffnung Auslösung des Lichtdetektors **5** – einerseits ein Augenscheinschutz der Anordnung und andererseits ein Berührungsschutz der eingeschlossenen Detektoren erreicht wird.

Das Gehäuse **7** ist in diesem Fall vorzugsweise elektromagnetisch abschirmend – Plaste mit Kupfer- und Eisenbeschichtung – ausgeführt und enthält innen eine die nachfolgenden Baugruppen abschirmende Bleiplatte **71**. Es kann auch nur vollständig als Bleigehäuse ausgeführt sein.

Die Wirkungsweise wird nach folgend beschrieben.

Wird die gesamte Anordnung mit Röntgenstrahlen bestrahlt und/oder anderen elektromagnetischen Feldern ausgesetzt, so ist auf Grund der Beschaffenheit des Gehäuses **7** nichts erkennbar und der Röntgenstrahlen-Detektor **6** bleibt inaktiv. Das Gehäuse **7** dient in erster Linie als Schutz bei Routineuntersuchungen durch den Zoll oder andere Kontrolldienste. Wenn sichergestellt ist, daß derartige Untersuchungen für das Gerät unterbleiben, kann das Gehäuse **7** weggelassen werden. Ist das Gehäuse **7** abgenommen und der Teil mit der Hülle **3** wird mit Röntgenstrahlen behandelt, so werden der Röntgenstrahlen-Detektor **6** aktiviert und demzufolge die sicherheitsrelevanten Daten verfälscht beziehungsweise gelöscht.

Bei dem Versuch mittels Aufbohren der Hülle **3** werden sowohl der Lichtdetektor **5** als auch der Leiter **4** ausgelöst und die sicherheitsrelevanten Daten in analoger Weise wie vorstehend beschrieben unkenntlich und damit für weitere Zwecke unmanipulierbar gemacht. Da der Lichtdetektor **5** mit einem Lichtleiter **51** gekoppelt ist, der die gesamte Oberfläche abdecken kann, ist jeglicher Lichteinfall wirksam.

Schließlich bildet bereits die erste innere Hülle **2** eine sichere Sperre gegen Röntgenuntersuchungen.

Bezugszeichenliste

1 Sicherheitsmodul
11 Modulplatine
2 Hülle aus Gießharz mit Röntgenstrahlen absorbierendem Füllstoff
3 lichtundurchlässige Hülle
4 mäanderförmiger elektrischer Leiter
5 Lichtdetektor
51 Lichtleiter
6 Röntgenstrahlen-Detektor
7 Röntgenstrahlen absorbierendes Gehäuse
71 Röntgenstrahlen absorbierende Platte im Gehäuse 7
8 Platine
9 Manipulationsschaltung
10 Batterie

Patentansprüche

1. Anordnung für einen Sicherheitsmodul zur Verhinderung des Auslesens oder der unberechtigten Manipulation sicherheitsrelevanter Daten, **dadurch gekennzeichnet,**
daß der Sicherheitsmodul (1) mindestens von einer Röntgenstrahlen absorbierenden Hülle (2) umgeben und
mit Mitteln (4, 5, 6) zur gezielten Manipulation sicherheitsrelevanter Daten bei mechanischem Eingriff und/oder Röntgenbestrahlung versehen ist.
2. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß die Hülle (2) aus Blei besteht.
3. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß die Hülle (2) aus einem Gießharz mit einem Röntgenstrahlen absorbierenden Füllstoff aus Blei- und Kupfer-Verbindungen sowie wahlweise weiteren Füllstoffen besteht.
4. Anordnung nach Anspruch 3, dadurch gekennzeichnet, daß eine Mischung aus 85% Mennige -Pb_3O_4- und 15% Cuprit -Cu_2O- und als weitere Füllstoffe wahlweise Quarzpulver, Glaskugeln oder Glasfaser eingesetzt sind.
5. Anordnung nach Anspruch 1, dadurch gekennzeichnet,
daß der Sicherheitsmodul (1) von einer weiteren, lichtundurchlässigen Hülle (3) umgeben ist und
daß im Übergangbereich zwischen dieser Hülle (3) und der Röntgenstrahlen absorbierenden Hülle (2) wahlweise ein mäanderförmiger elektrischer Leiter (4) oder ein Lichtdetektor (5) nebst Lichtleiter (51) oder ein Röntgenstrahlen-Detektor (6) oder Kombinationen derselben angeordnet sind, die mit dem Sicherheitsmodul (1) direkt oder über eine Manipulationsschaltung (9) elektrisch verbunden sind.
6. Anordnung nach Anspruch 1 und 5, dadurch gekennzeichnet, daß die Hülle (3) von einem Röntgenstrahlen absorbierenden Gehäuse (7) umgebeben ist, das auf eine Platine (8) aufgesetzt ist, die mit dem Sicherheitsmodul (1) elektrisch verbunden ist.
7. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß die Manipulationsschaltung (9) nur bei spannungslosem Zustand des Sicherheitsmoduls (1) mit demselben elektrisch verbunden ist.

Hierzu 1 Seite(n) Zeichnungen

Num :
Int. Cl.[6]:
Offenlegungstag:

DE 198 16 572 A1
G 06 K 19/00
14. Oktober 1999